ネットワークの脅威に対する組織の対策

広島大学 AI・データイノベーション教育研究センター
村上 祐子

目標

情報セキュリティに留意してネットワークサービスを安全に利用するために組織が注意すべき点を指摘できるようになる

この授業で紹介すること

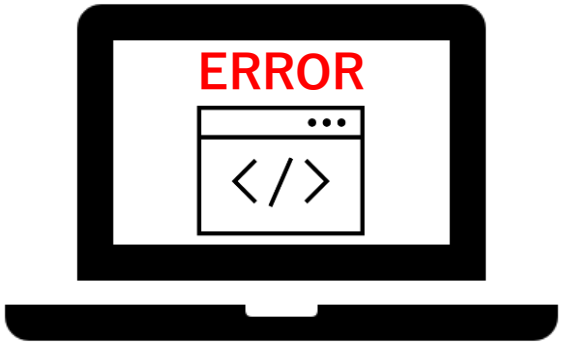
- 情報セキュリティを定義する３つの性質を理解する
- 組織がデータや情報を守るために適切な行動

キーワード

情報セキュリティ、機密性、完全性、可用性、ランサムウェア

こんなことはありませんか？

「大学のサイトに突然アクセスできなくなった」



組織はどのように対応するか？

- サイトメンテナンス中
  →メンテナンス前に学生に分かりやすく広報する
- 予期していない事象
  - 事故
  - 悪意を持った第３者による犯罪

情報を管理する「組織」が安全に情報をやりとりするには何に注意すべきか？

情報セキュリティ

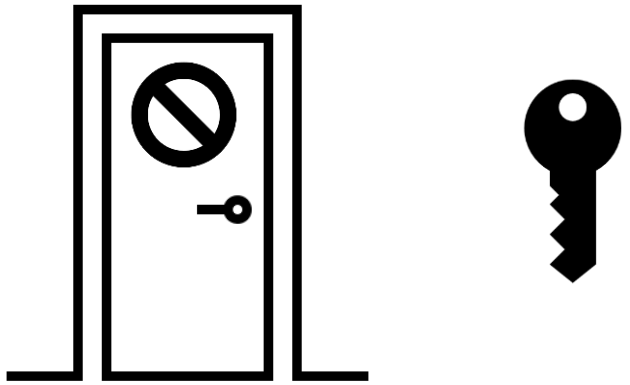
情報セキュリティは３つの性質を維持すること (ISO/IEC 27000)
- 機密性：情報へアクセスが認められた人だけが情報にアクセスできる
- 完全性：情報が破壊、改ざん、消去されない状態が保持されていること
- 可用性：情報へのアクセスを認められた人だけが必要な時に情報にアクセスできる

拡張した定義
- 真正性：操作、システムなどが主張どおりであることが確実である
- 責任追跡性：ある行為を誰が行ったか始めから終わりまで追跡できる
- 否認防止：動作や起きたことを後になって確認できて否認されない
- 信頼性：意図した通りにシステムが動作する

機密性の例

機密性を保持するために：

- 物理的な制限
  - 「関係者以外立ち入り禁止」
- 情報システムへのアクセス制限
  - 学生：自分の成績は閲覧できる
  - 教員：自分の担当する授業を受けている学生の情報は閲覧できる

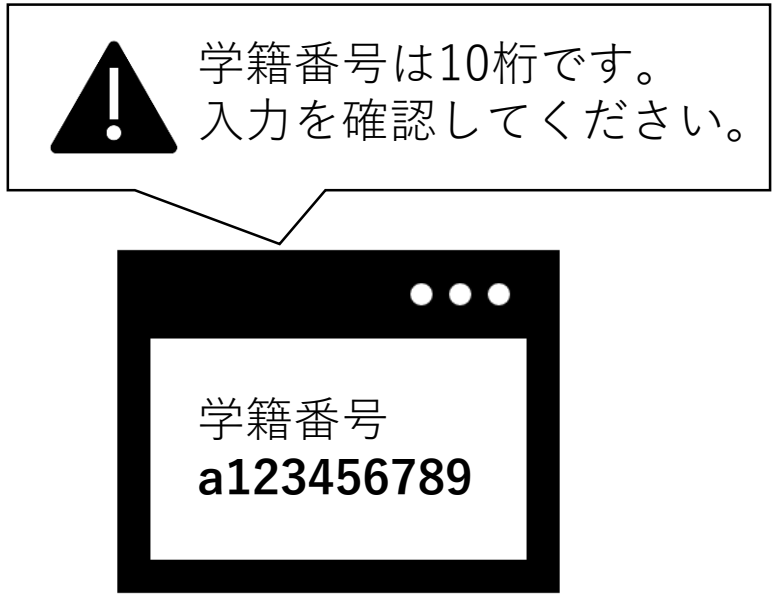


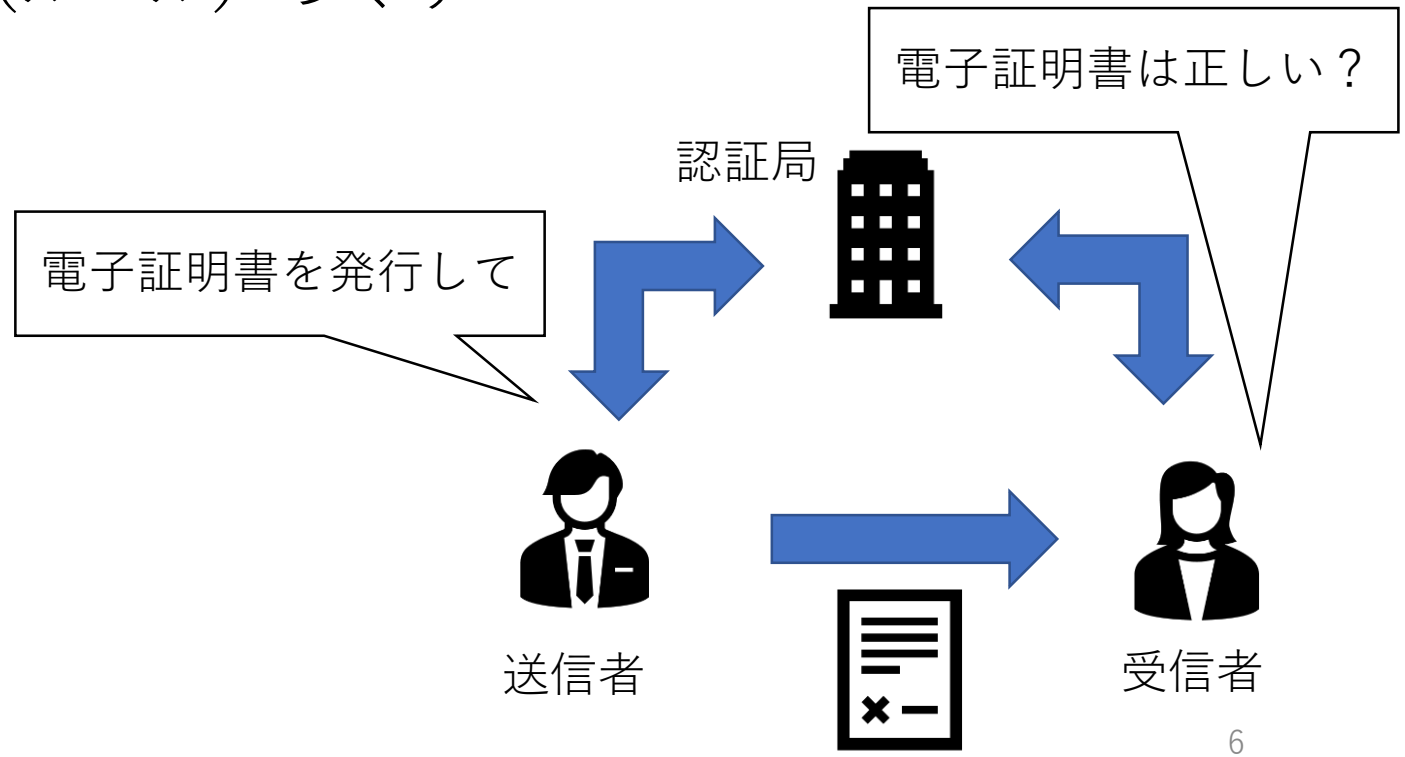
完全性の例

- 学生名簿の氏名、学籍番号、連絡先が正しく記録されている

完全性を保持するために：

- 入力ミスなどを防ぐシステム（ルール）づくり
- 電子署名



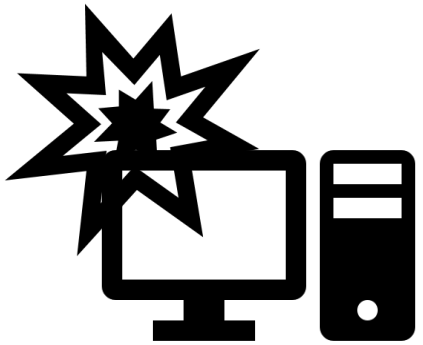


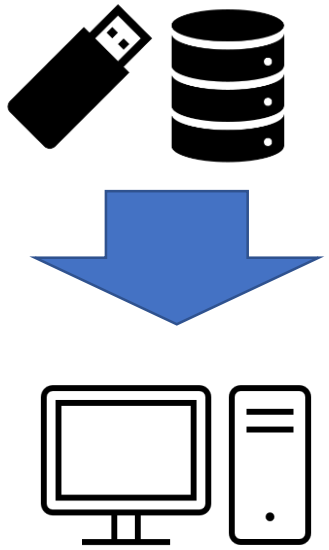
可用性の例

- 学生は在学期間中に大学のWebサイトで自分の成績を確認できる
  - 予告なくWebサイトにアクセスできなくなるのは可用性が喪失されている

可用性を保持するために：

- 情報を管理している機器の定期的な整備
- バックアップを定期的に取る





組織としての情報セキュリティ対策

- 情報管理の方法や体制、緊急時の対応をルール化する
  - ルールは組織の構成員が常に理解している状況にする
  - 組織の規模や業務内容を考慮して運営しやすいものにする
- 企業・組織のネットワークへの侵入対策
  - OS、アプリケーションを最新の状態にする
  - ウィルス対策ソフトを導入し常に最新の状態を保つ
- データ・システムのバックアップ
  - バックアップ装置、媒体はバックアップ時のみパソコンに接続する
  - バックアップから情報を復元できることを定期的に確認する

例題

大学２年生のあなたはサークル構成員の名簿管理の役職に就くことになりました。大学の規定により毎年６月に構成員名簿を大学に提出する必要があります。今年は後輩の1年生が4人サークルに所属することになりました。大学への報告が必要なことを直前まで忘れていたあなたは、とりあえず昨年度提出した名簿を大学に提出しました。

問題１

情報セキュリティの３つの性質のうち、どの性質が脅かされているでしょうか。

問題２

上記のような問題の発生を防ぐ対策を挙げてみましょう。

解説

問題１：「完全性」の喪失

大学２年生のあなたは…（中略）…とりあえず昨年度提出した名簿を大学に提出しました。

サークルの名簿が最新状態で登録されていない

→正しい情報ではない

問題２：解答例

- 名簿の管理者を増やす
- 大学に提出する前にサークル内で確認する規則を作る

ランサムウェア

デバイスに保存されているデータを暗号化して使用できないようにして、データを復旧するために金銭などを要求する攻撃手法

<u>近年の特徴</u>

- 企業・組織に対象を定めて攻撃する
- 確実に金銭を払わせるように手口が巧妙化
  - 企業・組織のネットワークに侵入し、重要な情報が保存されている場所を狙って感染させる
  - データを事前に搾取し「金銭支払がなければデータを公開する」などの脅迫を行う

問題

ランサムウェアに感染することによって、機密性、完全性、可用性のそれぞれがどのように脅かされるでしょうか。具体例を挙げて説明してください。